

Sabita J. Soneji, California Bar No. 224262
ssoneji@tzlegal.com

TYCKO & ZAVAREEI LLP

1970 Broadway

Suite 1070

Oakland, CA 94612

Telephone: (510) 254-6808

Katherine M. Aizpuru, *pro hac vice to be filed*

kaizpuru@tzlegal.com

TYCKO & ZAVAREEI LLP

2000 Pennsylvania Avenue NW

Suite 1010

Washington, D.C. 20006

Telephone: (202) 973-0900

Facsimile: (202) 973-0950

Attorneys for Plaintiffs and the Proposed Classes

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

ERIC ANDERSON, TIFFANY
MOORE, and DEKIMA THOMAS, *on
behalf of themselves and all others who are
similarly situated,*

Plaintiffs,

v.

TICKETMASTER LLC, and LIVE
NATION ENTERTAINMENT, INC.,

Defendants.

Case No. 2:24-cv-04709

**CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL**

1 Plaintiffs Eric Anderson, Tiffany Moore, and Dekima Thomas bring this Class
2 Action Complaint, both individually and on behalf of all others similarly situated,
3 against Defendants Live Nation Entertainment, Inc., and Ticketmaster LLC
4 (collectively, “Ticketmaster”). Plaintiffs’ allegations are based on personal knowledge
5 and belief and the investigation of counsel.

6 **INTRODUCTION**

7 1. Ticketmaster is by far the largest concert ticketing company in the United
8 States. Every year, Ticketmaster markets and sells billions of dollars’ worth of tickets
9 for live entertainment events to millions of consumers across the United States and
10 around the world.

11 2. As part of its business model, Ticketmaster collects and maintains
12 personally identifiable information, including, at a minimum, names, addresses, phone
13 numbers, and credit card information, (“PII”) from its hundreds of millions of
14 customers. Ticketmaster retains customers’ PII not just to facilitate the sale of
15 individual event tickets to individual customers, but for its own business interests and
16 profits—including marketing, market research, and advertising.

17 3. And Ticketmaster recognizes the tremendous responsibility it assumes in
18 each transaction that includes consumer PII, promising customers who “trust us with
19 your personal information” that Ticketmaster will “protect your information.”
20 Ticketmaster claims that its “goal” is to “maintain your trust and confidence by handling
21 your personal information with respect and putting you in control.”

22 4. But in May 2024, Ticketmaster failed to “protect” the information of over
23 half a billion customers worldwide who entrusted it with their PII, including names,
24 addresses, phone numbers, and certain credit card information. Threat actors breached
25 Ticketmaster’s computer systems and data, stole consumers’ PII (the “Data Breach”),
26 and advertised the stolen data for resale on the Dark Web.

27 5. Plaintiffs are loyal Ticketmaster customers, who, like millions of other
28 similarly situated persons, trusted Ticketmaster with personal information while

1 purchasing tickets to events. Now, Plaintiffs bring this class action lawsuit for
2 Ticketmaster's failure to adequately secure and protect its customers' PII.

3 6. By receiving and retaining Plaintiffs' and the Class Members' PII for its
4 own financial benefit, Ticketmaster assumed a duty to Plaintiffs and the Class Members
5 to implement and maintain reasonable and adequate security measures to secure,
6 protect, and safeguard Plaintiffs' and Class members' PII against unauthorized access
7 and disclosure.

8 7. Ticketmaster also had a duty to adequately safeguard this PII under
9 controlling case law, industry standards, and statutory obligations, including Section 5
10 of the Federal Trade Commission Act (the "FTC Act").

11 8. Ticketmaster breached those duties by, among other things, failing to
12 implement and maintain reasonable security procedures and practices to protect the PII
13 in its possession from unauthorized access and disclosure.

14 9. The Data Breach was directly traceable to Ticketmaster's failure to
15 implement adequate and reasonable cybersecurity procedures and protocols necessary
16 to protect consumers' private information. Ticketmaster disregarded the rights of
17 Plaintiffs and the Class Members by, among other things, neglecting to implement
18 adequate and reasonable measures to secure their data systems against unauthorized
19 intrusions; withholding disclosure regarding insufficiently robust computer systems and
20 security practices to safeguard PII; omitting standard and reasonably available steps to
21 prevent the Data Breach; inadequately training its staff and employees on proper
22 security measures; and failing to promptly and adequately notify Plaintiffs and the Class
23 Members of the Data Breach.

24 10. Furthermore, Ticketmaster neglected proper monitoring of the computer
25 network and systems containing the PII. If Ticketmaster had conducted adequate
26 monitoring, it could have detected the intrusion sooner or potentially prevented it
27 altogether.

28 11. To date, there is no indication that Ticketmaster has notified customers

1 of the specifics surrounding the breach, including the full scope of the breach and the
2 reasons it occurred. Instead, Ticketmaster prioritized notifying its shareholders by
3 quickly filing a form with the Securities & Exchange Commission, in which it admitted
4 the unauthorized access.

5 12. As a result of the Data Breach, Plaintiffs and the Class Members have
6 suffered measurable losses, including the diminished value of their bargain, out-of-
7 pocket expenses, and the value of the time reasonably spent to address or mitigate the
8 effects of the attack. Additionally, they have experienced emotional distress and face
9 the substantial risk of future harm due to the compromise of their PII.

10 13. The Data Breach has exposed Plaintiffs and the Class Members to an
11 immediate and impending threat of fraud and identity theft. As a precaution, they must
12 diligently monitor their financial accounts to thwart potential identity theft.
13 Additionally, they will need to bear out-of-pocket expenses for purchasing essential
14 credit monitoring, identity theft protection and insurance services, credit freezes, credit
15 reports, or other protective measures to prevent and detect identity theft, both now and
16 in the future.

17 14. As a result, Plaintiffs and the Class Members will need to allocate extra
18 time to review credit reports and oversee their financial accounts for signs of fraud or
19 identity theft. Given the exposure of other unchangeable personal details, the threat of
20 identity theft and fraud will endure throughout their lifetimes.

21 15. Although accessed and reportedly exfiltrated by unauthorized criminal
22 actors, Plaintiffs' and the Class Members' sensitive PII still resides within Ticketmaster's
23 possession. Without additional safeguards and independent review, this information
24 remains susceptible to further cyberattacks and theft.

25 16. Plaintiffs' and the Class Members' identities face significant jeopardy due
26 to Ticketmaster's wrongful actions, as the PII Ticketmaster collected is now in the
27 possession of data thieves. This ongoing risk will persist throughout their lifetimes.

28

JURISDICTION AND VENUE

17. This Court has original subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) the amount in controversy exceeds \$5 million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiffs, have different citizenships from the defendants.

18. This Court has personal jurisdiction over both Defendants because both Defendants have purposefully availed themselves of the laws, rights, and benefits of the State of California. Each Defendant is headquartered in California and has engaged in activities including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district; (ii) conducting substantial business in this forum; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in California and in this judicial District.

19. This Court has supplemental jurisdiction to hear all state law statutory and common law claims pursuant to 28 U.S.C. § 1367.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Ticketmaster is based in this District, maintains Plaintiffs' and the Class Members' PII in this District, and has caused harm to Plaintiffs and the Class Members in this District.

PARTIES

Plaintiff Eric Anderson

21. At all relevant times, Plaintiff Eric Anderson is and has been a citizen of the State of New York.

22. As early as 2011, Plaintiff Anderson created an account on Ticketmaster's website to purchase event tickets. Plaintiff Anderson provided his PII during the registration process.

1 23. Since creating his account, Plaintiff Anderson has made at least 20 ticket
2 purchases using his Ticketmaster account.

3 24. Plaintiff Anderson's account remains active.

4 25. Plaintiff Anderson is deeply concerned about the Data Breach, as his PII
5 may now be readily available for cybercriminals to sell, buy, or exchange on the Dark
6 Web.

7 26. Since learning about the Data Breach, Plaintiff Anderson has spent several
8 hours researching the incident to determine its extent and gravity. He anticipates
9 spending substantial additional time to mitigate future damages, including reviewing his
10 existing accounts for fraudulent activity and closely monitoring his financial
11 information.

12 27. Plaintiff Anderson has a continuing interest in ensuring that his PII, which
13 remains in Ticketmaster's possession, is protected, and safeguarded from future
14 breaches.

15 **Plaintiff Tiffany Moore**

16 28. At all relevant times, Plaintiff Tiffany Moore is and has been a citizen of
17 the State of Illinois.

18 29. Since at least 2012, Plaintiff Moore has maintained an account on
19 Ticketmaster's website to purchase event tickets, providing her PII during the
20 registration process.

21 30. Since creating her account, Plaintiff Moore has made at least 50 ticket
22 purchases using her Ticketmaster account.

23 31. Plaintiff Moore's account remains active.

24 32. Plaintiff Moore is deeply concerned about the Data Breach, as her PII may
25 now be readily available for cybercriminals to sell, buy, or exchange on the Dark Web.

26 33. Since learning about the Data Breach, Plaintiff Moore has spent several
27 hours researching the incident to determine its extent and gravity. She anticipates
28 spending substantial additional time to mitigate future damages, including reviewing her

1 existing accounts for fraudulent activity and closely monitoring her financial
2 information.

3 34. Plaintiff Moore has a continuing interest in ensuring that her PII, which
4 remains in Ticketmaster's possession, is protected, and safeguarded from future
5 breaches.

6 **Plaintiff Dekima Thomas**

7 35. At all relevant times, Plaintiff Dekima Thomas is and has been a citizen
8 of the District of Columbia.

9 36. Since at least 2013, Plaintiff Thomas has maintained an account on
10 Ticketmaster's website to purchase event tickets, providing her PII during the
11 registration process.

12 37. Since creating her account, Plaintiff Thomas has made at least 12 ticket
13 purchases using her Ticketmaster account.

14 38. Plaintiff Thomas's account remains active.

15 39. Plaintiff Thomas is deeply concerned about the Data Breach, as her PII
16 may now be readily available for cybercriminals to sell, buy, or exchange on the Dark
17 Web.

18 40. Since learning about the Data Breach, Plaintiff Thomas has spent several
19 hours researching the incident to determine its extent and gravity. She anticipates
20 spending substantial additional time to mitigate future damages, including reviewing her
21 existing accounts for fraudulent activity and closely monitoring her financial
22 information.

23 41. Plaintiff Thomas has a continuing interest in ensuring that her PII, which
24 remains in Ticketmaster's possession, is protected, and safeguarded from future
25 breaches.

26 **Defendant Ticketmaster LLC**

27 42. Defendant Ticketmaster LLC is a wholly owned subsidiary of Live Nation
28 Entertainment, Inc.

43. Ticketmaster LLC is a limited liability company organized and existing under the laws of Virginia with its principal place of business in Beverly Hills, California.

44. Plaintiffs and the Class Members are current and former customers of Ticketmaster and account holders on Ticketmaster.com.

45. Due to the nature of the services Ticketmaster provides, it receives and is entrusted with securely storing customers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information.

46. Ticketmaster promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

Defendant Live Nation Entertainment, Inc.

47. Defendant Live Nation Entertainment, Inc. ("Live Nation") is a Delaware corporation headquartered in Beverly Hills, California.

48. Live Nation is the world's largest entertainment company, facilitating connections among over half a billion fans across its platforms in 29 countries. In 2023, it boasted revenues of approximately \$22.7 billion.¹

FACTUAL ALLEGATIONS

A. Ticketmaster Chooses to Collect and Keep User's Private Information

49. Ticketmaster controls about 70% of the market for ticketing services for live entertainment events. Individuals looking to buy and sell tickets for most major sporting, entertainment, theater and other events are thus forced to use Ticketmaster's services. Consumers wanting to attend events often have no choice but to purchase tickets through Ticketmaster. Indeed, the Department of Justice has recently filed an

¹ Jem Aswad, *Live Nation Posts Another Record Year in 2023, Revenue Up 36% to Almost \$23 Billion*, Variety (Feb. 22, 2024), <https://variety.com/2024/music/news/live-nation-2023-earnings-record-year-1235919844/>.

1 antitrust case against Ticketmaster for its anticompetitive practices.

2 50. Ticketmaster requires consumers who purchase tickets on their platform
3 to provide their PII to Ticketmaster, both to facilitate the ticket sales and also for
4 Ticketmaster's own business purposes. Ticketmaster promises to keep consumers' PII
5 secure.

6 51. Data security purportedly forms a crucial aspect of Ticketmaster's
7 business model. For instance, on a segment of Ticketmaster LLC's website, the
8 company declares:

9 "Our goal is to maintain your trust and confidence by
10 handling your personal information with respect and putting
11 you in control...As a global company, our fans are located
12 all over the world, depending on your market there are
13 specific laws and regulations around privacy rights such as
14 the GDPR in Europe, LGPD in Brazil and CCPA in United
15 States...We have security measures in place to protect your
16 information."²

17 52. Live Nation also maintains a privacy policy section, affirming its
18 adherence to various international data privacy frameworks and the laws of the United
19 States.³

20 53. Plaintiffs and the Class Members entrusted their PII to Ticketmaster with
21 the reasonable expectation and mutual understanding that Ticketmaster would fulfill its
22 obligations to maintain the confidentiality and security of such information,
23 safeguarding it against unauthorized access.

24 **B. Ticketmaster Failed To Protect that Private Information**

25 54. Despite Ticketmaster's explicit assurances that it would employ
26 reasonable measures to safeguard its customers' sensitive PII, and only share that
27 information with expressly authorized individuals, an "unauthorized" person or
28

² Ticketmaster, Privacy Policy, <https://privacy.ticketmaster.com/privacy-policy> (last accessed June 4, 2024).

³ Live Nation Entertainment Privacy Policy, <https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy> (last accessed June 4, 2024).

1 persons accessed Ticketmaster's network servers and reportedly stole the PII they
2 found there.

3 55. Ticketmaster neglected to secure the PII of individuals who entrusted it
4 with sensitive PII. Ticketmaster failed to undertake appropriate measures to shield the
5 PII of Plaintiffs and other Class Members from unauthorized disclosure.

6 56. On May 20, 2024, Ticketmaster identified unauthorized activity within its
7 databases containing Ticketmaster data.

8 57. A week later, infamous cybercrime group ShinyHunters posted an
9 advertisement for the stolen Ticketmaster PII on the dark web—claiming to have
10 obtained 1.3 terabytes of Ticketmaster user data, including names, addresses, phone
11 numbers, order details, and partial credit card information for approximately 560
12 million customers.⁴ ShinyHunters is reportedly demanding a payment of approximately
13 \$500,000.⁵

14 58. ShinyHunters is a criminal group known for engaging in audacious
15 hacking sprees, then selling trove after trove of freshly stolen data on the dark web.⁶
16 ShinyHunters has been linked to a string of high-profile data breaches, resulting in
17 millions of dollars of losses. In 2020, the group claimed to have stolen data from nearly
18 a dozen websites ranging from an Indonesian ecommerce platform to the Minnesota
19 *Star Tribune* newspaper, a dating app, a meal kit company, the *Chronicle of Higher*
20 *Education*, and Microsoft's private Github account. The following year, the group sold
21 a database of stolen information from 70 million AT&T customers. And in September
22 of last year, ShinyHunters stole data for nearly 200,000 Pizza Hut customers.

23 59. In 2022, a French citizen was arrested for his involvement with
24 ShinyHunters, extradited to the United States to face prosecution. He was sentenced to
25

26 ⁴ Juliana Kim, *Ticketmaster hack may affect more than 500 million customers*, NPR (June 1, 2024),
27 <https://www.npr.org/2024/06/01/nx-s1-4988602/ticketmaster-cyber-attack-million-customers>.

28 ⁵ *Id.*

⁶ Lily Hay Newman, *ShinyHunters is a Hacking Group on a Data Breach Spree*, Wired (May 21, 2020),
<https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/>.

1 three years in prison and ordered to pay more than \$5 million in restitution.⁷

2 60. Ticketmaster did not immediately respond to reports of the data breach
3 and the reported disclosure of its customers' sensitive information. Ticketmaster
4 refused even to confirm the hack to reporters.

5 61. But on May 31, 2024, Ticketmaster notified shareholders via a filing with
6 the Securities & Exchange Commission that it was aware of the breach and had
7 "launched an investigation with industry-leading forensic investigators to understand
8 what happened."

9 62. As of June 5, 2024, Ticketmaster still has neither issued a formal statement
10 to the public nor notified its customers regarding the compromise of their PII, which
11 is likely in the possession of cybercriminals.

12 63. Consequently, Plaintiffs and the Class Members remain uninformed,
13 unaware of the potential exploitation of their PII for identity theft, phishing scams, and
14 other cybercrimes, which could and often do lead to compromised credit scores and
15 related consequences.

16 64. If, as ShinyHunters claims (and Ticketmaster has not, to date, disputed),
17 it is true that the Ticketmaster data breach included information from 560 million
18 customers worldwide, it would be one of the most significant data breaches ever in
19 terms of numbers and the extent of the data stolen.

20 65. Ticketmaster is no stranger to data privacy issues. In 2020, Ticketmaster
21 agreed to pay a \$10 million fine after admitting it hacked into one of its competitors.⁸
22 And in November of last year, Ticketmaster was allegedly hit by a cyber attack that
23 affected sales of tickets for the Taylor Swift Eras tour.⁹

24
25
26 ⁷ Annika Burgess, *What we know about the 'remarkably devious' ShinyHunters hackers allegedly behind the*
Ticketmaster data leak, ABC News Australia (May 31, 2024), [https://www.abc.net.au/news/2024-05-](https://www.abc.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928)
27 [31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928](https://www.abc.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928).

28 ⁸ BBC, *Ticketmaster confirms hack which could affect 560m* (June 2, 2024),
<https://www.bbc.com/news/articles/cw99ql0239wo>.

⁹ *Id.*

C. Ticketmaster Failed to Comply with FTC Guidelines

66. The FTC Act, 15 U.S.C. § 45, prohibits Ticketmaster from committing “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (“FTC”) has determined that a company’s failure to uphold reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act.

67. The FTC has issued guidelines for businesses emphasizing the significance of adopting reasonable data security practices. According to the FTC, integrating data security considerations into all aspects of business decision-making is imperative. A

68. In 2016, the FTC issued an updated version of its publication, “Protecting Personal Information: A Guide for Business,” which established cyber-security guidelines for businesses.¹⁰ These guidelines underscored the importance for businesses to safeguard personal customer information, securely dispose of unnecessary personal data, encrypt information stored on computer networks, assess network vulnerabilities, and institute policies to address security issues promptly. Additionally, the guidelines recommend using intrusion detection systems to promptly detect breaches, monitoring incoming traffic for signs of hacking attempts, being vigilant about large data transmissions, and having a response plan prepared in the event of a breach.¹¹

69. The FTC also advises that companies not retain PII longer than necessary for transaction authorization, restrict access to sensitive data, enforce the use of complex passwords on networks, employ industry-tested security methods, monitor the network for suspicious activity, and ensure that third-party service providers have implemented adequate security measures.

70. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ

¹⁰ Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

¹¹ *Id.*

1 reasonable and appropriate measures to protect against unauthorized access to
2 confidential consumer data as an unfair act or practice.

3 71. Ticketmaster failed to properly implement basic data security practices by
4 failing to employ reasonable and appropriate measures to protect against unauthorized
5 access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of
6 the FTC Act, 15 U.S.C. § 45.

7 72. Ticketmaster was at all times fully aware of the obligation to protect the
8 PII of customers and patients. Ticketmaster was also aware of the significant
9 repercussions that would result from their failure to do so.

10 **D. Ticketmaster Failed to Comply with Industry Standards**

11 73. Large, prominent companies like Ticketmaster are particularly vulnerable
12 to cyberattacks because of the sensitive nature of the information that they collect and
13 maintain. Because of this vulnerability, and because of the frequency and scale of data
14 breaches in recent years, companies like Ticketmaster that routinely handle and
15 maintain sensitive customer information should, at a minimum, implement industry
16 best practices.

17 74. These practices include educating and training employees; requiring
18 strong passwords and multi-factor authentication for employees and users;
19 implementing multi-layer security like firewalls, antivirus programs, and anti-malware
20 software; limiting access to sensitive data; backing up and encrypting data; setting up
21 network firewalls; monitoring and limiting network ports; and monitoring and limiting
22 access to physical security systems.

23 75. Ticketmaster failed to meet the minimum standards of any of the
24 following frameworks laying out industry best practices: the NIST Cybersecurity
25 Framework Version 1.1 (including at a minimum PR.AC-1, PR.AC-3, PR.AC-4,
26 PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3,
27 DE.CM-1, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's
28 Critical Security Controls (CIS CSC), which are all established standards in reasonable

1 cybersecurity readiness.

2 76. These frameworks represent the established industry norms for data
3 security, and Ticketmaster's failure to adhere to these widely accepted standards caused
4 the Data Breach and has provided an avenue for criminal exploitation.

5 **E. Plaintiffs and the Class Suffered and Face Substantial Risk of Future**
6 **Injuries Because Ticketmaster Failed to Protect Their Private**
7 **Information**

8 77. As a result of Ticketmaster's failure to implement and adhere to security
9 measures that would have protected their PII, Ticketmaster customer PII is now in the
10 hands of unauthorized third parties, which may include thieves, unknown criminals,
11 banks, credit companies, and other potentially malicious individuals. Consequently,
12 Plaintiffs and the Class Members, who are Ticketmaster customers and provided their
13 PII to Ticketmaster, now face an elevated risk of identity theft. They will need to expend
14 significant time and money to protect themselves, both now and in the future, due to
15 Ticketmaster's Data Breach.

16 78. Plaintiffs and other Class Members have had their personal and sensitive
17 PII exposed to the public, resulting in ongoing emotional pain, mental anguish, and
18 embarrassment.

19 79. As a result of the Data Breach, Plaintiffs and the Class Members face an
20 increased risk of identity theft, phishing attacks, and related cybercrimes. Those affected
21 are experiencing heightened and prolonged anxiety and fear, knowing they will be
22 vulnerable to cybercrimes for years to come.

23 80. PII is a valuable property right. Due to its significant value and the
24 prevalence of large-scale data breaches, identity thieves and cybercriminals have openly
25 posted credit card numbers, Social Security numbers, PII, and other sensitive
26 information on various internet websites, making it publicly accessible. Information
27 from multiple breaches, including the Data Breach, can be aggregated, increasing its
28 value to thieves and amplifying the potential harm to victims.

81. PII can be sold at prices exceeding \$1,000.¹² A stolen credit or debit card number can sell for \$15 to \$110 on the Dark Web.¹³ Criminals can also purchase access to entire company data breaches for an average cost of between \$2,000 to \$4,000.¹⁴

82. Law-abiding consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”¹⁵

83. Accordingly, any company that conducts business with a consumer and subsequently compromises the privacy of their PII effectively deprives that consumer of the full monetary value of their transaction with the company.

84. Cyberattacks have become so prevalent that the FBI and U.S. Secret Service have issued warnings to potential targets, urging them to be aware of and prepared for potential attacks.¹⁶

85. Therefore, Plaintiffs and the Class Members must now immediately allocate time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on sensitive accounts more frequently; (3) rigorously screen phone calls, emails, and other

¹² Ryan Smith, *Revealed – How much is Personal information worth on the dark web?*, Insurance News (May 1, 2023), <https://www.insurancebusinessmag.com/us/news/breaking-news/revealed-how-much-is-personal-information-worth-on-the-dark-web-444453.aspx>.

¹³ Miklos Zoltan, *Dark Web Price Index 2023*, Privacy Affairs (April 23, 2023), <https://www.privacyaffairs.com/dark-web-price-index-2023/>.

¹⁴ Kaspersky, *Cybercriminals sell access to companies via the Dark Web from \$2000* (June 15, 2022), https://www.kaspersky.com/about/press-releases/2022_cybercriminals-sell-access-to-companies-via-the-dark-web-from-2000.

¹⁵ Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, An Experimental Study, 22(2) Information Systems Research 254 (June 2011), accessible at <https://www.jstor.org/stable/23015560?seq=1>.

¹⁶ Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974>.

1 communications to avoid social engineering or spear phishing attacks; and (4) search
2 for and subscribe to suitable identity theft protection and credit monitoring services.

3 86. Once PII is exposed, it is nearly impossible to ensure the information is
4 fully recovered or protected from future misuse.

5 87. As a result, Plaintiffs and the Class Members will need to maintain these
6 heightened protective measures for years, possibly their entire lives, due to
7 Ticketmaster's actions. Additionally, the value of Plaintiffs' and the Class Members' PII
8 has been diminished by its exposure in the Data Breach.

9 88. Thus, due to Ticketmaster's failures, Plaintiffs and the Class Members face
10 a substantial risk of suffering identity theft, fraud, and misuse of their PII, including but
11 not limited to: (a) damage to and diminution in the value of their PII, a form of property
12 that Ticketmaster obtained from Plaintiffs and the Class; (b) violation of their privacy
13 rights; and (c) ongoing and increased risk of identity theft and fraud.

14 **CLASS ACTION ALLEGATIONS**

15 89. Plaintiffs propose the following Class and Subclass definitions, subject to
16 amendment(s) as appropriate:

17 **Nationwide Class:**

18 **All residents of the United States whose personal**
19 **information was compromised due to the data breach.**

20 **District of Columbia Subclass:**

21 **All citizens of the District of Columbia whose personal**
22 **information was compromised due to the data breach.**

23 **Illinois Subclass:**

24 **All citizens of Illinois whose personal information was**
25 **compromised due to the data breach.**

26 **New York Subclass:**

27 **All citizens of New York whose personal information**
28 **was compromised due to the data breach.**

1 90. The Nationwide Class (“Class”) and Subclasses are collectively referred to as
2 the Classes.

3 91. Excluded from the Classes are Ticketmaster’s officers and directors, and
4 any entity in which Ticketmaster LLC or Live Nation have a controlling interest; and
5 Ticketmaster’s affiliates, legal representatives, attorneys, successors, heirs, and assigns.
6 Excluded also from the Class are members of the judiciary to whom this case is assigned,
7 their families, and members of their staff.

8 92. Plaintiffs reserve the right to amend or modify the Class or Subclass
9 definitions as this case progresses.

10 93. Numerosity: Upon information and belief, the members of the Class are
11 so numerous that joinder of all of them is impracticable.

12 94. Predominance of Common Questions of Fact and Law: There are
13 questions of law and fact common to the Class, which predominate over any
14 questions affecting only individual Class Members. These common questions of law and
15 fact include, without limitation:

- 16 a. Whether Ticketmaster unlawfully utilized, retained, misplaced, or exposed
17 Plaintiffs’ and the Class Members’ PII.
- 18 b. Whether Ticketmaster neglected to establish and uphold reasonable
19 security protocols and practices commensurate with the nature and scale
20 of the data compromised in the Data Breach.
- 21 c. Whether Ticketmaster’s data security measures preceding and during the
22 Data Breach adhered to relevant data security laws and regulations.
- 23 d. Whether Ticketmaster’s data security measures preceding and during the
24 Data Breach aligned with industry norms and standards.
- 25 e. Whether Ticketmaster had an obligation to Class Members to protect their
26 PII.
27
28

- f. Whether Ticketmaster were subject to (and violated) the FTC Act.
- g. Whether Ticketmaster breached their obligations to Class Members to safeguard their PII.
- h. Whether malicious actors accessed Class Members' PII in the Data Breach.
- i. Whether Ticketmaster was aware or reasonably should have been aware of deficiencies in their data security systems and monitoring procedures.
- j. Whether Ticketmaster's actions constituted negligence.
- k. Whether Ticketmaster's failure to abide by its statutory duties to Plaintiffs and the Class Members was negligence per se.
- l. Whether Ticketmaster formed express or implied contracts with the Plaintiffs and the Class Members to protect their PII.
- m. Whether Ticketmaster breached its express or implied contracts with Plaintiffs and the Class Members.
- n. Whether Ticketmaster was unjustly enriched at the expense of Plaintiffs and the Class.
- o. Whether Ticketmaster violated the District of Columbia Consumer Protection Procedures Act.
- p. Whether Ticketmaster violated the Illinois Personal Information Protection Act.
- q. Whether Ticketmaster violated the Illinois Consumer Fraud and Deceptive Business Practices Act.
- r. Whether Ticketmaster violated the Illinois Uniform Deceptive Trade Practices Act.
- s. Whether Ticketmaster violated the New York General Business Law §

1 349.

2 t. Whether Ticketmaster violated the California Consumer Privacy Act.

3 u. Whether Ticketmaster violated the California Consumer Legal Remedies
4 Act.

5 v. Whether Ticketmaster violated the California Unfair Competition Law.

6 w. Whether Ticketmaster failed to promptly provide notice of the Data
7 Breach, and

8 x. Whether Plaintiffs and the Class Members are entitled to compensatory
9 damages, statutory damages, treble damages, punitive damages, and/or
10 injunctive relief.

11 95. Typicality: Plaintiffs' claims are typical of those of other Class Members
12 because Plaintiffs' PII, like that of every other Class Member, were compromised in the
13 Data Breach.

14 96. Adequacy: Plaintiffs are adequate representatives for the Class and Subclasses
15 because their interests do not conflict with the interests of the Class that they seek to
16 represent. Plaintiffs have retained counsel competent and highly experienced in
17 complex class action litigation—including consumer fraud and privacy class action
18 cases—and counsel intends to prosecute this action vigorously. The interests of the
19 Class will be fairly and adequately protected by Plaintiffs and their experienced counsel.

20 97. Superiority: A class action is superior to all other available means of fair
21 and efficient adjudication of the claims of Plaintiffs and members of the Class. The
22 injury suffered by each individual Class Member is relatively small in comparison to the
23 burden and expense of individual prosecution of the complex and extensive litigation
24 necessitated by Ticketmaster's conduct. It would be virtually impossible for members
25 of the Class individually to redress effectively the wrongs done to them by Ticketmaster.
26 Even if Class Members could afford such individual litigation, the court system could
27 not. Individualized litigation presents a potential for inconsistent or contradictory
28

1 judgments. Individualized litigation increases the delay and expense to all parties, and
 2 to the court system, presented by the complex legal and factual issues of the case. By
 3 contrast, the class action device presents far fewer management difficulties, and provides
 4 the benefits of single adjudication, an economy of scale, and comprehensive supervision
 5 by a single court. Upon information and belief, members of the Class can be readily
 6 identified and notified based upon, inter alia, the records (including databases, e-mails,
 7 dealership records and files, etc.) Ticketmaster maintains regarding their consumers.

8 **COUNT I**

9 ***Negligence***

10 **(On Behalf of Plaintiffs and the Class)**

11 98. Plaintiffs reallege and incorporate by reference all preceding paragraphs as
 12 if fully set forth herein.

13 99. Ticketmaster owed a duty to Plaintiffs and all other Class Members to
 14 exercise reasonable care in safeguarding and protecting their PII in its possession,
 15 custody, or control.

16 100. Ticketmaster knew, or should have known, the risks associated with
 17 collecting and storing Plaintiffs' and all other Class Members' PII, as well as the critical
 18 importance of maintaining secure systems. Ticketmaster was aware, or should have
 19 been aware, of the significant increase in data breaches in recent years. Consequently,
 20 Ticketmaster had a duty to protect the PII of Plaintiffs and the Class Members.

21 101. Given the nature of its business, the sensitivity and value of the PII it
 22 maintains, and the resources at its disposal, Ticketmaster should have identified
 23 vulnerabilities in its systems and taken measures to prevent the Data Breach, a duty it
 24 was obligated to uphold.

25 102. Ticketmaster breached its duties by failing to exercise reasonable care in
 26 safeguarding and protecting Plaintiffs' and the Class Members' PII. Specifically,
 27 Ticketmaster failed to design, implement, manage, monitor, and audit appropriate data
 28 security processes, controls, policies, procedures, protocols, and software and hardware

1 systems necessary to protect the PII entrusted to it, including that of Plaintiffs and the
2 Class Members.

3 103. It was reasonably foreseeable to Ticketmaster that failure to exercise
4 reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' PII
5 by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and
6 audit appropriate data security processes, controls, policies, procedures, protocols, and
7 software and hardware systems would result in the unauthorized release, disclosure, and
8 dissemination of Plaintiffs' and the Class Members' PII to unauthorized individuals.

9 104. But for Ticketmaster's negligent conduct or breach of the above-
10 described duties owed to Plaintiffs and the Class Members, their PII would not have
11 been compromised.

12 105. As a result of Ticketmaster's wrongful actions, inaction, and lack of
13 ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all
14 other Class Members have suffered, and will continue to suffer, damages and other
15 harm, including but not limited to: (i) a substantially increased risk of identity theft,
16 necessitating expenditures for protective and remedial services for which they are
17 entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the
18 confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is
19 a well-established national and international market; (v) lost time and money spent
20 mitigating and remediating the effects of the Data Breach, including the increased risks
21 of identity theft they face and will continue to face; and (vi) actual or attempted fraud.

22 **COUNT II**
23 ***Negligence Per Se***
24 **(On Behalf of Plaintiffs and the Class)**

25 106. Plaintiffs reallege and incorporate by reference all preceding paragraphs as
26 if fully set forth herein.

27 107. Ticketmaster's duties arise from Section 5 of the FTCA, 15 U.S.C. §
28 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce." The FTC
interprets this to include the unfair practice by a business, such as Ticketmaster, of

1 failing to employ reasonable measures to protect and secure PII.

2 108. Ticketmaster violated Section 5 of the FTCA by failing to use reasonable
3 measures to protect Plaintiffs' and the Class Members' PII and by not complying with
4 applicable industry standards. Ticketmaster's conduct was particularly unreasonable
5 given the nature and volume of the PII it collects and stores, as well as the foreseeable
6 consequences of a data breach, including the substantial damages that would result for
7 Plaintiffs and the Class Members.

8 109. Ticketmaster's violations of Section 5 of the FTCA constitute negligence
9 per se.

10 110. Plaintiffs and the Class Members are within the class of persons that
11 Section 5 of the FTCA were intended to protect.

12 111. The harm resulting from the Data Breach is precisely the type of harm
13 that Section 5 of the FTCA were designed to prevent.

14 112. It was reasonably foreseeable to Ticketmaster that failing to exercise
15 reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' PII—
16 by not designing, adopting, implementing, controlling, directing, overseeing, managing,
17 monitoring, and auditing appropriate data security processes, controls, policies,
18 procedures, protocols, and software and hardware systems—would result in the release,
19 disclosure, and dissemination of Plaintiffs' and the Class Members' PII to unauthorized
20 individuals.

21 113. The injury and harm suffered by Plaintiffs and the other Class Members
22 were the direct and proximate results of Ticketmaster's violations of Section 5 of the
23 FTCA. Plaintiffs and the Class Members have suffered, and will continue to suffer,
24 damages and other actual harm, including but not limited to: (i) a substantially increased
25 risk of identity theft, necessitating expenditures for protective and remedial services for
26 which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach
27 of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which
28 there is a well-established national and international market; (v) lost time and money

1 spent mitigating and remediating the effects of the Data Breach; and (vi) actual or
2 attempted fraud.

3 **COUNT III**
4 ***Breach Of Contract***
5 **(On Behalf of Plaintiffs and the Class)**

6 114. Plaintiffs reallege and incorporate by reference all allegations of the
7 preceding factual allegations as though fully set forth herein.

8 115. Ticketmaster required Plaintiffs and the Class Members to provide, or
9 authorize the transfer of, their PII for Ticketmaster to provide services. In exchange,
10 Ticketmaster entered into contracts with Plaintiffs and the Class Members, wherein
11 Ticketmaster agreed to protect Plaintiffs' and the Class Members' PII.

12 116. Ticketmaster made the following express promises to Plaintiffs and the
13 Class Members in the privacy policy on the Ticketmaster LLC website:

- 14 • "You trust us with your personal information, so we strive to always be
15 clear and honest about how and why we will use it."
- 16 • "Our goal is to maintain your trust and confidence by handling your
17 personal information with respect and putting you in control."
- 18 • "We're always taking steps to make sure your information is protected and
19 deleted securely when we no longer need it. . . . This information is
20 regularly deleted."
- 21 • "We have security measures in place to protect your information."
- 22 • Ticketmaster promised only to share Plaintiffs and the Class Members'
23 PII with specific persons—Event Partners and Commercial Partners as
24 defined in the contract, specific vendors identified in the contract, and
25 relevant local government officials—not unauthorized third parties.
- 26 • Ticketmaster promised that Plaintiffs and the Class Members' PII would
27 only be used for specific purposes—Ticketmaster's "legitimate business
28 interests"—not unauthorized uses.

117. Ticketmaster made the following express promises to Plaintiffs and the

1 Class Members in the privacy policy on the Live Nation website:

- 2 • “Please note that we will never use or disclose sensitive personal
- 3 information you give us except to provide you with the goods and services
- 4 you have requested or for the limited purposes allowed under the law.”
- 5 • “[W]e will use the information you provide us to fulfill our obligations to
- 6 you in delivering that service and, where permitted, keep you up to date
- 7 about other events that may be of interest to you[.]” In other words,
- 8 information would not be used for other purposes.
- 9 • Ticketmaster promised that it would only use Plaintiffs’ and the Class
- 10 Members’ PII “as disclosed and described here.”
- 11 • Ticketmaster promised that it would only share Plaintiffs’ and the Class
- 12 Members’ PII with third parties identified in the contract, and that it
- 13 would notify Plaintiffs and the Class Members before sharing their
- 14 information “for reasons not described in this policy.”
- 15 • “In all situations, your personal data will be securely deleted after the
- 16 relevant limitation or retention periods have expired.”
- 17 • “We have security measures in place to protect your information.”

18 118. These promises to Plaintiffs and the Class Members formed the basis of
 19 the bargain between Plaintiffs and the Class Members, on the one hand, and
 20 Ticketmaster, on the other.

21 119. Plaintiffs and the Class Members would not have provided their PII to
 22 Ticketmaster had they known that Ticketmaster would not safeguard their PII.

23 120. Plaintiffs and the Class Members fully performed their obligations under
 24 their contracts with Ticketmaster.

25 121. Ticketmaster breached their contracts with Plaintiffs and the Class
 26 Members by failing to safeguard Plaintiffs and the Class Members’ PII.

27 122. As a direct and proximate result of Ticketmaster’s breaches of its contracts
 28 with Plaintiffs and the Class Members, Plaintiffs and the Class Members have suffered,

1 and will continue to suffer, economic damages and other actual harm, including but not
 2 limited to: (i) a substantially increased risk of identity theft, necessitating expenditures
 3 for protective and remedial services for which they are entitled to compensation; (ii)
 4 improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv)
 5 deprivation of the value of their PII, for which there is a well-established national and
 6 international market; (v) lost time and money spent mitigating and remediating the
 7 effects of the Data Breach; and (vi) actual or attempted fraud.

8 **COUNT IV**

9 ***In the Alternative—Breach of Implied Contract*** **(On Behalf of Plaintiffs and the Class)**

10 123. Plaintiffs reallege and incorporate by reference all allegations of the
 11 preceding factual allegations as though fully set forth herein.

12 124. Plaintiffs allege Count IV in the alternative to Count III above.

13 125. Ticketmaster required Plaintiffs and the Class Members to provide, or
 14 authorize the transfer of, their PII for Ticketmaster to provide services. In exchange,
 15 Ticketmaster entered into implied contracts with Plaintiffs and the Class Members,
 16 wherein Ticketmaster agreed to adhere to their statutory and common law duties to
 17 protect Plaintiffs' and the Class Members' PII, and to promptly notify them in the event
 18 of a data breach.

19 126. Plaintiffs and the Class Members would not have provided their PII to
 20 Ticketmaster had they known that Ticketmaster would not safeguard their PII, as
 21 promised, or provide timely notice of a data breach.

22 127. Plaintiffs and the Class Members fully performed their obligations under
 23 their implied contracts with Ticketmaster.

24 128. Ticketmaster breached the implied contracts by failing to safeguard
 25 Plaintiffs and the Class Members' PII and by failing to provide them with timely and
 26 accurate notice of the Data Breach.

27 129. As a direct and proximate result of Ticketmaster's breaches of its implied
 28 contracts with Plaintiffs and the Class Members, Plaintiffs and the Class Members have

suffered, and will continue to suffer, damages and other actual harm, including but not limited to: (i) a substantially increased risk of identity theft, necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money spent mitigating and remediating the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT V

In the Alternative—Unjust Enrichment **(On Behalf of Plaintiffs and the Class)**

130. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

131. Plaintiffs allege Count V in the alternative to Count III above.

132. Plaintiffs and the Class Members provided Ticketmaster with a monetary benefit through payments made for production services or other services.

133. Ticketmaster accepted or was aware of the benefits conferred upon it by Plaintiffs and the Class Members. Additionally, Ticketmaster benefitted from receiving Plaintiffs' and the Class Members' PII.

134. Due to Ticketmaster's actions, Plaintiffs and the Class Members incurred actual damages equivalent to the disparity in value between the payments made for services with reasonable data privacy and security measures that Plaintiffs and the Class Members expected, and the services received lacking such measures.

135. Ticketmaster should not be permitted to retain the money belonging to Plaintiffs and the Class Members because Ticketmaster failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and the Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

136. Ticketmaster should be compelled to disgorge all unlawfully obtained proceeds resulting from the conduct and Data Breach alleged herein for the benefit of

1 Plaintiffs and the Class Members.

2 **COUNT VI**

3 ***Violation of the District of Columbia Consumer Protection Procedures Act***

4 **D.C. Code §§ 28-3901 *et seq.***

5 **(On Behalf of Plaintiff Thomas and the District of Columbia Subclass)**

6 137. Plaintiff Thomas realleges and incorporates all previous allegations as
7 though fully set forth herein.

8 138. Plaintiff Thomas brings this claim on behalf of herself and the District of
9 Columbia (“D.C.”) Subclass.

10 139. Plaintiff Thomas and the D.C. Subclass Members are “consumers” as
11 defined in the District of Columbia Consumer Protection Procedures Act (“CPPA”),
12 D.C. Code § 28-3901(a)(2).

13 140. Ticketmaster engaged in deceptive acts or practices in violation of the
14 CPPA, including:

15 a. Failing to implement and maintain reasonable security and privacy
16 measures to protect Plaintiff Thomas’s and the D.C. Subclass Members’ PII,
17 which was a direct and proximate cause of the Data Breach;

18 b. Failing to identify and remediate foreseeable security and privacy
19 risks and sufficiently improve security and privacy measures despite knowing the
20 risk of cybersecurity incidents, which was a direct and proximate cause of the
21 Data Breach;

22 c. Failing to comply with common law and statutory duties pertaining
23 to the security and privacy of Plaintiff Thomas’s and the D.C. Subclass Members’
24 PII, including the duties imposed by the FTC Act, 15 U.S.C. § 45, which was a
25 direct and proximate cause of the Data Breach;

26 d. Misrepresenting that it would protect Plaintiff Thomas’s and the
27 D.C. Subclass Members’ PII, including by implementing and maintaining
28 reasonable security measures;

e. Misrepresenting that it would comply with common law and

1 statutory duties pertaining to the security and privacy of Plaintiff Thomas's and
2 the D.C. Subclass Members' PII, including duties imposed by the FTC Act, 15
3 U.S.C. § 45;

4 f. Omitting, suppressing, and concealing the material fact that it did
5 not properly secure Plaintiff Thomas's and the D.C. Subclass Members' PII;

6 g. Omitting, suppressing, and concealing the material fact that it did
7 not comply with common law and statutory duties pertaining to the security and
8 privacy of Plaintiff Thomas's and the D.C. Subclass Members' PII, including
9 duties imposed by the FTC Act, 15 U.S.C. § 45; and

10 h. Misrepresenting that Plaintiff Thomas's and the D.C. Subclass
11 Members' transactions with Ticketmaster conferred or offered rights, remedies,
12 or obligations that it did not have, including that Ticketmaster would protect
13 Plaintiff Thomas's and the D.C. Subclass Members' PII.

14 141. Ticketmaster's representations and omissions were material because they
15 were likely to deceive reasonable consumers about the adequacy of Ticketmaster's data
16 security and its ability to protect Plaintiff Thomas's and the D.C. Subclass Members'
17 PII.

18 142. As a direct and proximate result of Ticketmaster's unlawful and deceptive
19 acts and practices, Plaintiff Thomas and the D.C. Subclass Members have suffered, and
20 will continue to suffer, damages and other actual and ascertainable losses of money or
21 property, and monetary and non-monetary damages and harm, including but not limited
22 to: (i) a substantially increased risk of identity theft, necessitating expenditures for
23 protective and remedial services for which they are entitled to compensation; (ii)
24 improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv)
25 deprivation of the value of their PII, for which there is a well-established national and
26 international market; (v) lost time and money spent mitigating and remediating the
27 effects of the Data Breach; and (vi) actual or attempted fraud.

28 143. The above deceptive and unlawful practices and acts by Ticketmaster

1 caused substantial injury to Plaintiff Thomas and the D.C. Subclass Members that they
2 could not have reasonably avoided.

3 144. Plaintiff Thomas and the D.C. Subclass Members seek all monetary and
4 non-monetary relief allowed by law, including actual and statutory damages, treble
5 damages, injunctive relief, and attorneys' fees and costs.

6 **COUNT VII**

7 ***Violation of the Illinois Personal Information Protection Act***

8 **815 Ill. Comp. Stat. §§ 530/10(a) *et seq.***

9 **(On Behalf of Plaintiff Moore and the Illinois Subclass)**

10 145. Plaintiff Moore realleges and incorporates all previous allegations as though
11 fully set forth herein.

12 146. Plaintiff Moore brings this claim on behalf of herself and the Illinois
13 Subclass.

14 147. As a publicly held corporation which handles, collects, disseminates, and
15 otherwise deals with nonpublic PII, Ticketmaster is a Data Collector as defined in the
16 Illinois Personal Information Protection Act ("ILPIPA"), 815 Ill. Comp. Stat. § 530/5.

17 148. Ticketmaster is a Data Collector that owns or licenses computerized data
18 that includes PII. Ticketmaster also maintains computerized data that includes PII that
19 Ticketmaster does not own.

20 149. Plaintiff Moore's and the Illinois Subclass Members' PII includes
21 "Personal Information" as defined by 815 Ill. Comp. Stat. § 530/5.

22 150. The ILPIPA requires Ticketmaster to give immediate notice of breach of
23 a security system to owners of Personal Information that Ticketmaster does not own
24 or license, including Plaintiff Moore and the Illinois Subclass Members.

25 151. Ticketmaster failed to give immediate notice of the Data Breach to
26 Plaintiff Moore and the Illinois Subclass Members. That failure violated 815 Ill. Comp.
27 Stat. § 530/10(b).

28 152. The ILPIPA also requires Ticketmaster to notify Plaintiff Moore and the
Illinois Subclass Members of a breach of its data security system that may have

1 compromised Personal Information which Ticketmaster owns or licenses in the most
2 expedient time possible and without unreasonable delay.

3 153. Ticketmaster failed to provide notice of the Data Breach to Plaintiff
4 Moore and the Illinois Subclass Members expediently and without unreasonable delay.
5 That failure violated 815 Ill. Comp. Stat. § 530/10(a).

6 154. Violating ILPIPA is an unlawful practice under the Illinois Consumer
7 Fraud and Deceptive Business Practices Act.

8 155. As a direct and proximate result of Ticketmaster's violations of ILPIPA,
9 Plaintiff Moore and the Illinois Subclass Members have suffered, and will continue to
10 suffer, damages and other actual and ascertainable losses of money or property, and
11 monetary and non-monetary damages and harm, including but not limited to: (i) a
12 substantially increased risk of identity theft, necessitating expenditures for protective
13 and remedial services for which they are entitled to compensation; (ii) improper
14 disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of
15 the value of their PII, for which there is a well-established national and international
16 market; (v) lost time and money spent mitigating and remediating the effects of the
17 Data Breach; and (vi) actual or attempted fraud.

18 156. Plaintiff Moore and the Illinois Subclass Members seek relief under 815
19 Ill. Comp. Stat. § 510/3 for the harm they suffered due to Ticketmaster's violations of
20 ILPIPA, including equitable relief, costs, and attorneys' fees.

21 **COUNT VIII**

22 ***Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act***
23 **815 Ill. Comp. Stat. §§ 505 *et seq.***

24 **(On Behalf of Plaintiff Moore and the Illinois Subclass)**

25 157. Plaintiff Moore realleges and incorporate all previous allegations as though
26 fully set forth herein.

27 158. Plaintiff Moore brings this claim on behalf of herself and the Illinois
28 Subclass.

159. Ticketmaster is a "person" as defined by the Illinois Consumer Fraud and

1 Deceptive Business Practices Act (“ICFA”), 815 Ill. Comp. Stat. § 505/1(c).

2 160. Plaintiff Moore and the Illinois Subclass Members are “consumers” as
3 defined by 815 Ill. Comp. Stat. § 505/1(e).

4 161. Ticketmaster’s conduct as described in this Complaint was in the conduct
5 of “trade” or “commerce” as defined in 815 Ill. Comp. Stat. § 505/1(f).

6 162. Ticketmaster engaged in deceptive acts or practices in the conduct of its
7 trade or commerce in violation of the ICFA, including:

8 a. Failing to implement and maintain reasonable security and privacy
9 measures to protect Plaintiff Moore’s and the Illinois Subclass Members’ PII,
10 which was a direct and proximate cause of the Data Breach;

11 b. Failing to identify and remediate foreseeable security and privacy
12 risks and sufficiently improve security and privacy measures despite knowing the
13 risk of cybersecurity incidents, which was a direct and proximate cause of the
14 Data Breach;

15 c. Failing to comply with common law and statutory duties pertaining
16 to the security and privacy of Plaintiff Moore’s and the Illinois Subclass
17 Members’ PII, including the duties imposed by the FTC Act, 15 U.S.C. § 45, the
18 Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a),
19 and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*, which was a direct and
20 proximate cause of the Data Breach;

21 d. Misrepresenting that it would protect Plaintiff Moore’s and the
22 Illinois Subclass Members’ PII, including by implementing and maintaining
23 reasonable security measures;

24 e. Misrepresenting that it would comply with common law and
25 statutory duties pertaining to the security and privacy of Plaintiff Moore’s and
26 the Illinois Subclass Members’ PII, including duties imposed by the FTC Act, 15
27 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp.
28 Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*;

1 f. Omitting, suppressing, and concealing the material fact that it did
2 not properly secure Plaintiff Moore's and the Illinois Subclass Members' PII; and

3 g. Omitting, suppressing, and concealing the material fact that it did
4 not comply with common law and statutory duties pertaining to the security and
5 privacy of Plaintiff Moore's and the Illinois Subclass Subclass Members' PII,
6 including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform
7 Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA,
8 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*

9 163. Ticketmaster's representations and omissions were material because they
10 were likely to deceive reasonable consumers about the adequacy of Ticketmaster's data
11 security and its ability to protect Plaintiff Moore's and the Illinois Subclass Members'
12 PII.

13 164. The above unfair and deceptive practices and acts by Ticketmaster were
14 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
15 to Plaintiff Moore and the Illinois Subclass that they could not reasonably avoid; and
16 the substantial injury outweighed any benefits to consumers or to competition.

17 165. As a direct and proximate result of Ticketmaster's unlawful and deceptive
18 acts and practices, Plaintiff Moore and the Illinois Subclass Members have suffered, and
19 will continue to suffer, damages and other actual and ascertainable losses of money or
20 property, and monetary and non-monetary damages and harm, including but not limited
21 to: (i) a substantially increased risk of identity theft, necessitating expenditures for
22 protective and remedial services for which they are entitled to compensation; (ii)
23 improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv)
24 deprivation of the value of their PII, for which there is a well-established national and
25 international market; (v) lost time and money spent mitigating and remediating the
26 effects of the Data Breach; and (vi) actual or attempted fraud.

27 166. Plaintiff Moore and the Illinois Subclass Members seek all monetary and
28 non-monetary relief allowed by law, including damages, restitution, punitive damages,

1 injunctive relief, and attorneys' fees and costs.

2 **COUNT IX**

3 ***Violation of the Illinois Uniform Deceptive Trade Practices Act***

4 **815 Ill. Comp. Stat. §§ 510/1 *et seq.***

5 **(On Behalf of Plaintiff Moore and the Illinois Subclass)**

6 167. Plaintiff Moore realleges and incorporates all previous allegations as though
7 fully set forth herein.

8 168. Plaintiff Moore brings this claim on behalf of herself and the Illinois
9 Subclass.

10 169. Ticketmaster is a "person" as defined by the Illinois Uniform Deceptive
11 Trade Practices Act ("IUDTPA"), 815 Ill. Comp. Stat. § 510/1(5).

12 170. Ticketmaster engaged in deceptive trade practices in the conduct of its
13 business, in violation of 815 Ill. Comp. Stat. § 510/2(a), including:

14 a. Representing that goods or services have characteristics they do not
15 have;

16 b. Representing that goods or services are of a particular standard,
17 quality, or grade if they are of another;

18 c. Advertising goods or services with intent not to sell them as
19 advertised; and

20 d. Engaging in other conduct that creates a likelihood of confusion or
21 misunderstanding.

22 171. Ticketmaster's deceptive acts and practices include:

23 a. Failing to implement and maintain reasonable security and privacy
24 measures to protect Plaintiff Moore's and the Illinois Subclass Members' PII,
25 which was a direct and proximate cause of the Data Breach;

26 b. Failing to identify and remediate foreseeable security and privacy
27 risks and sufficiently improve security and privacy measures despite knowing the
28 risk of cybersecurity incidents, which was a direct and proximate cause of the
Data Breach;

1 c. Failing to comply with common law and statutory duties pertaining
 2 to the security and privacy of Plaintiff Moore's and the Illinois Subclass
 3 Members' PII, including the duties imposed by the FTC Act, 15 U.S.C. § 45, the
 4 IUDTPA, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat.
 5 §§ 530/10(a) *et. seq.*, which was a direct and proximate cause of the Data Breach;

6 d. Misrepresenting that it would protect Plaintiff Moore's and the
 7 Illinois Subclass Members' PII, including by implementing and maintaining
 8 reasonable security measures;

9 e. Misrepresenting that it would comply with common law and
 10 statutory duties pertaining to the security and privacy of Plaintiff Moore's and
 11 the Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15
 12 U.S.C. § 45, the IUDTPA, 815 Ill. Comp. Stat. § 510/2(a), and the ILPIPA, 815
 13 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*;

14 f. Omitting, suppressing, and concealing the material fact that it did
 15 not properly secure Plaintiff Moore's and the Illinois Subclass Members' PII; and

16 g. Omitting, suppressing, and concealing the material fact that it did
 17 not comply with common law and statutory duties pertaining to the security and
 18 privacy of Plaintiff Moore's and the Illinois Subclass Subclass Members' PII,
 19 including duties imposed by the FTC Act, 15 U.S.C. § 45, the IUDTPA, 815 Ill.
 20 Comp. Stat. § 510/2(a), and the ILPIPA, 815 Ill. Comp. Stat. §§ 530/10(a) *et. seq.*

21 172. Ticketmaster's representations and omissions were material because they
 22 were likely to deceive reasonable consumers about the adequacy of Ticketmaster's data
 23 security and its ability to protect Plaintiff Moore's and the Illinois Subclass Members'
 24 PII.

25 173. The above unfair and deceptive practices and acts by Ticketmaster were
 26 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
 27 to Plaintiff Moore and the Illinois Subclass that they could not reasonably avoid; and
 28 the substantial injury outweighed any benefits to consumers or to competition.

174. As a direct and proximate result of Ticketmaster's unlawful and deceptive acts and practices, Plaintiff Moore and the Illinois Subclass Members have suffered, and will continue to suffer, damages and other actual and ascertainable losses of money or property, and monetary and non-monetary damages and harm, including but not limited to: (i) a substantially increased risk of identity theft, necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money spent mitigating and remediating the effects of the Data Breach; and (vi) actual or attempted fraud.

175. Plaintiff Moore and the Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief.

COUNT X

Violation of the New York General Business Law § 349

N.Y. Gen. Bus. Law § 349

(On Behalf of Plaintiff Anderson and the New York Subclass)

176. Plaintiff Anderson realleges and incorporates all previous allegations as though fully set forth herein.

177. Plaintiff Anderson brings this claim on behalf of himself and the New York Subclass.

178. Ticketmaster engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

i. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Anderson's and the New York Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

j. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the

1 Data Breach;

2 k. Failing to comply with common law and statutory duties pertaining
3 to the security and privacy of Plaintiff Anderson's and the New York Subclass
4 Members' PII, including the duties imposed by the FTC Act, 15 U.S.C. § 45,
5 which was a direct and proximate cause of the Data Breach;

6 l. Misrepresenting that it would protect Plaintiff Anderson's and the
7 New York Subclass Members' PII, including by implementing and maintaining
8 reasonable security measures;

9 m. Misrepresenting that it would comply with common law and
10 statutory duties pertaining to the security and privacy of Plaintiff Anderson's and
11 the New York Subclass Members' PII, including duties imposed by the FTC Act,
12 15 U.S.C. § 45;

13 n. Omitting, suppressing, and concealing the material fact that it did
14 not properly secure Plaintiff Anderson's and the New York Subclass Members'
15 PII; and

16 o. Omitting, suppressing, and concealing the material fact that it did
17 not comply with common law and statutory duties pertaining to the security and
18 privacy of Plaintiff Anderson's and the New York Subclass Members' PII,
19 including duties imposed by the FTC Act, 15 U.S.C. § 45.

20 179. Ticketmaster's representations and omissions were material because they
21 were likely to deceive reasonable consumers about the adequacy of Ticketmaster's data
22 security and its ability to protect Plaintiff Anderson's and the New York Subclass
23 Members' PII.

24 180. As a direct and proximate result of Ticketmaster's unlawful and deceptive
25 acts and practices, Plaintiff Anderson and the New York Subclass Members have
26 suffered, and will continue to suffer, damages and other actual and ascertainable losses
27 of money or property, and monetary and non-monetary damages and harm, including
28 but not limited to: (i) a substantially increased risk of identity theft, necessitating

1 expenditures for protective and remedial services for which they are entitled to
 2 compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of
 3 their PII; (iv) deprivation of the value of their PII, for which there is a well-established
 4 national and international market; (v) lost time and money spent mitigating and
 5 remediating the effects of the Data Breach; and (vi) actual or attempted fraud.

6 181. Ticketmaster's deceptive and unlawful acts and practices complained of
 7 herein affected the public interest and consumers at large, including the many New
 8 Yorkers affected by the Data Breach.

9 182. The above deceptive and unlawful practices and acts by Ticketmaster
 10 caused substantial injury to Plaintiff Anderson and the New York Subclass that they
 11 could not have reasonably avoided.

12 183. Plaintiff Anderson and the New York Subclass Members seek all
 13 monetary and non-monetary relief allowed by law, including actual and statutory
 14 damages, treble damages, injunctive relief, and attorneys' fees and costs.

15 **COUNT XI**

16 ***Violation of the California Consumer Privacy Act of 2018***

17 **Cal. Civ. Code §§ 1798.100 et seq.**

18 **(On Behalf of Plaintiffs and the Class)**

19 184. Plaintiffs reallege and incorporate all previous allegations as though fully set
 20 forth herein.

21 185. The Data Breach occurred within the State of California, where
 22 Ticketmaster LLC and Live Nation reside and where the acts and practices to which the
 23 Data Breach is directly traceable occurred.

24 186. As more personal information about consumers is collected by businesses,
 25 consumers' ability to properly protect and safeguard their privacy has decreased.
 26 Consumers entrust businesses with their personal information on the understanding
 27 that businesses will adequately protect it from unauthorized access.

28 187. As a result, in 2018, the California Legislature passed the CCPA, giving
 consumers broad protections and rights intended to safeguard their personal

1 information. Among other things, the CCPA imposes an affirmative duty on certain
2 businesses that maintain personal information about California residents to implement
3 and maintain reasonable security procedures and practices that are appropriate to the
4 nature of the information collected.

5 188. Ticketmaster is subject to the CCPA and failed to implement such
6 procedures, resulting in the Data Breach.

7 189. Section 1798.150(a)(1) of the CCPA provides: “Any consumer whose
8 nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject
9 to an unauthorized access and exfiltration, theft, or disclosure because of the business’
10 violation of the duty to implement and maintain reasonable security procedures and
11 practices appropriate to the nature of the information to protect the personal
12 information may institute a civil action for” statutory or actual damages, injunctive or
13 declaratory relief, and any other relief the court deems proper.

14 190. Plaintiffs are “consumers” as defined by Civ. Code § 1798.140(g) because
15 he is natural person residing in the state of California.

16 191. Ticketmaster is a “business” as defined by Civ. Code, § 1798.140(c).

17 192. The CCPA provides that “personal information” includes “[a]n
18 individual’s first name or first initial and the individual’s last name in combination with
19 any one or more of the following data elements, when either the name or the data
20 elements are not encrypted or redacted . . . (iii) Account number or credit or debit card
21 number, in combination with any required security code, access code, or password that
22 would permit access to an individual’s financial account.” *See* Civ. Code, §
23 1798.150(a)(1); Civ. Code, § 1798.81.5(d)(1)(A).

24 193. Plaintiffs’ PII compromised in the Data Breach constitutes “personal
25 information” within the meaning of the CCPA.

26 194. Through the Data Breach, Plaintiffs’ PII was accessed without
27 authorization, exfiltrated, and stolen by criminals.

28 195. The Data Breach occurred because of Ticketmaster’s failure to implement

1 and maintain reasonable security procedures and practices appropriate to the nature of
2 the information.

3 196. Simultaneously herewith, Plaintiffs are providing notice to Ticketmaster
4 pursuant to Civ. Code, § 1798.150(b)(1), identifying the specific provisions of the CCPA
5 that Plaintiffs allege Ticketmaster has violated or is violating. Although a cure is not
6 possible under the circumstances, if (as expected) Ticketmaster is unable to cure or do
7 not cure the violation within 30 days, Plaintiffs will amend this Complaint to pursue
8 actual or statutory damages as permitted by Civ. Code, § 1798.150(a)(1)(A)..

9 **COUNT XII**

10 ***Violation of the Consumer Legal Remedies Act***

11 **Cal. Civ. Code §§ 1750 et seq. (“CLRA”)**

12 **(On Behalf of Plaintiffs and the Class)**

13 197. Plaintiffs reallege and incorporate by reference every allegation contained
14 elsewhere in this Complaint as if fully set forth herein.

15 198. The Data Breach occurred within the State of California, where
16 Ticketmaster LLC and Live Nation reside and where the acts and practices to which the
17 Data Breach is directly traceable occurred.

18 199. This cause of action is brought pursuant to the California Consumers
19 Legal Remedies Act (the “CLRA”), Cal. Civ. Code § 1750, *et seq.* This cause of action
20 does not seek monetary damages currently but is limited solely to injunctive relief.
21 Plaintiffs will later amend this Complaint to seek damages in accordance with the CLRA
22 after providing Ticketmaster with notice required by Civ. Code, § 1782.

23 200. Plaintiffs and the Class Members are “consumers,” as the term is defined
24 by Cal. Civ. Code, § 1761(d).

25 201. Plaintiffs, Class Members and Ticketmaster have engaged in
26 “transactions,” as that term is defined by Civ. Code, § 1761(e).

27 202. The conduct alleged in this Complaint, which Ticketmaster committed in
28 California, constitutes unfair methods of competition and unfair and deceptive acts and
practices for the purpose of the CLRA including:

1 a. Representing that goods or services have characteristics or benefits
2 that they do not have;

3 b. Representing that goods or services are of a particular standard,
4 quality, or grade if they are of another;

5 c. Advertising goods or services with intent not to sell them as
6 advertised; and

7 d. Representing that a transaction confers or involves rights,
8 remedies, or obligations that it does not have or involve.

9 203. Ticketmaster's deceptive acts and practices include:

10 a. Failing to implement and maintain reasonable security and privacy
11 measures to protect Plaintiffs' and the Class Members' PII, which was a direct
12 and proximate cause of the Data Breach;

13 b. Failing to identify and remediate foreseeable security and privacy
14 risks and sufficiently improve security and privacy measures despite knowing the
15 risk of cybersecurity incidents, which was a direct and proximate cause of the
16 Data Breach;

17 c. Failing to comply with common law and statutory duties pertaining
18 to the security and privacy of Plaintiffs' and the Class Members' PII, including
19 the duties imposed by the FTC Act, 15 U.S.C. § 45, and the CCPA, which was a
20 direct and proximate cause of the Data Breach;

21 d. Misrepresenting that it would protect Plaintiffs' and the Class
22 Members' PII, including by implementing and maintaining reasonable security
23 measures;

24 e. Misrepresenting that it would comply with common law and
25 statutory duties pertaining to the security and privacy of Plaintiffs' and the Class
26 Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the
27 CCPA;

28 f. Omitting, suppressing, and concealing the material fact that it did

1 not properly secure Plaintiffs' and the Class Members' PII; and

2 g. Omitting, suppressing, and concealing the material fact that it did
3 not comply with common law and statutory duties pertaining to the security and
4 privacy of Plaintiffs' and the Class Members' PII, including duties imposed by
5 the FTC Act, 15 U.S.C. § 45, and the CCPA.

6 204. As a result of engaging in such conduct, Ticketmaster violated Civ. Code, §
7 1770.

8 205. Pursuant to Civil Code section 1780, subdivision (a)(2) and (a)(5), Plaintiffs
9 seek an order of this Court that includes, but is not limited to, an order enjoining
10 Ticketmaster from continuing to engage in unlawful, unfair, or fraudulent business
11 practices or any other act prohibited by law.

12 206. Plaintiffs and the Class Members suffered injuries caused by
13 Ticketmaster's misrepresentations, because they provided their PII believing that
14 Ticketmaster would adequately protect this information.

15 207. Plaintiffs and the Class Members may be irreparably harmed and/or
16 denied an effective and complete remedy if such an order is not granted.

17 208. The unfair and deceptive acts and practices of Ticketmaster, as described
18 above, present a serious threat to Plaintiffs and members of the Class.

19 **COUNT XIII**

20 ***Violation of the California Unfair Competition Law***

21 **Cal. Bus. and Prof. Code §§ 17200, et seq. ("UCL")**

22 **(On Behalf of Plaintiffs and the Class)**

23 209. Plaintiffs reallege and incorporate by reference all preceding factual
24 allegations as though fully set forth herein.

25 210. Plaintiffs bring this claim on behalf of themselves and the Class.

26 211. The Data Breach occurred within the State of California, where
27 Ticketmaster LLC and Live Nation reside and where the acts and practices to which the
28 Data Breach is directly traceable occurred.

212. The California Unfair Competition Law, Bus. & Prof. Code, §17200, *et seq.*

1 (“UCL”), prohibits any “unlawful,” “fraudulent” or “unfair” business act or practice and
2 any false or misleading advertising, as defined by the UCL and relevant case law.

3 213. By reason of Ticketmaster’s above-described wrongful actions, inaction,
4 and omissions, all of which occurred in California, the resulting Data Breach, and the
5 unauthorized disclosure of Plaintiffs’ and the Class Members’ PII, Ticketmaster
6 engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

7 214. Ticketmaster’s business practices as alleged herein are unfair because they
8 offend established public policy and are immoral, unethical, oppressive, unscrupulous,
9 and substantially injurious to consumers, in that the private and confidential PII of
10 consumers has been compromised for all to see, use, or otherwise exploit.

11 215. Ticketmaster’s practices were unlawful and in violation of the CCPA and
12 CLRA and Ticketmaster’s own privacy policies because Ticketmaster failed to take
13 reasonable measures to protect Plaintiffs’ and the Class Members’ PII.

14 216. Ticketmaster’s business practices as alleged herein are fraudulent because
15 they are likely to deceive consumers into believing that the PII they provide to
16 Ticketmaster will remain private and secure, when in fact it was not private and secure.

17 217. Plaintiffs and the Class Members suffered (and continue to suffer) injury
18 in fact and lost money or property as a direct and proximate result of Ticketmaster’s
19 above- described wrongful actions, inaction, and omissions including, *inter alia*, the
20 unauthorized release and disclosure of their PII.

21 218. Ticketmaster’s above-described wrongful actions, inaction, and omissions,
22 the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs’ and
23 the Class Members’ PII also constitute “unfair” business acts and practices within the
24 meaning of Bus. & Prof. Code, § 17200 *et seq.*, in that Ticketmaster’s conduct was
25 substantially injurious to Plaintiffs and the Class Members, offensive to public policy,
26 immoral, unethical, oppressive, and unscrupulous, and the gravity of Ticketmaster’s
27 conduct outweighs any alleged benefits attributable to such conduct.

28 219. But for Ticketmaster’s misrepresentations and omissions, Plaintiffs and

1 the Class Members would not have provided their PII to Ticketmaster or would have
 2 insisted that their PII be more securely protected.

3 220. As a direct and proximate result of Ticketmaster's above-described
 4 wrongful actions, inaction, and omissions, the resulting Data Breach, and the
 5 unauthorized release and disclosure of Plaintiffs' and the Class Members' PII, they have
 6 been injured as follows: (1) the loss of the opportunity to control how their PII is used;
 7 (2) the diminution in the value and/or use of their PII entrusted to Ticketmaster; (3) the
 8 increased, imminent risk of fraud and identity theft; (4) the compromise, publication,
 9 and/or theft of their PII; and (5) costs associated with monitoring their PII, amongst
 10 other things.

11 221. Plaintiffs take upon themselves enforcement of the laws violated by
 12 Ticketmaster in connection with the reckless and negligent disclosure of PII. There is a
 13 financial burden incurred in pursuing this action and it would be against the interests of
 14 justice to penalize Plaintiffs by forcing them to pay attorneys' fees and costs from the
 15 recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate
 16 under California Code of Civil Procedure section 1021.5.

17 **PRAYER FOR RELIEF**

18 **WHEREFORE**, Plaintiffs, individually and on behalf of the Class, pray for
 19 judgment as follows:

- 20 a) An Order certifying this action as a class action and appointing
 21 Plaintiffs and their counsel to represent the Class and
 22 Subclasses as described above;
- 23 b) Equitable relief enjoining Defendants from engaging in the wrongful
 24 conduct complained of herein pertaining to the misuse and/or
 25 disclosure of Plaintiffs' and the Class Members' PII;
- 26 c) Equitable relief compelling Defendants to utilize appropriate methods
 27 and policies with respect to consumer data collection, storage, and
 28 safety, and to disclose with specificity the type of PII compromised

during the Data Breach;

- d) For an order requiring Defendants to pay for credit monitoring services for Plaintiffs and the Class of a duration to be determined at trial;
- e) An award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, and as allowable by law;
- f) An award of punitive damages, as allowable by law;
- g) An award of attorneys' fees and costs, and any other expense, including expert witness fees;
- h) Pre-judgment and post-judgment interest on any amounts awarded; and
- i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: June 5, 2024

By: /s/ Sabita J. Soneji
Sabita J. Soneji, Cal. Bar No. 224262
ssoneji@tzlegal.com
TYCKO & ZAVAREEI LLP
1970 Broadway
Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808

Katherine M. Aizpuru, *pro hac vice* forthcoming
kaizpuru@tzlegal.com
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue NW
Suite 1010
Washington, D.C. 20006
Telephone: (202) 973-0900
Facsimile: (202) 973-0950

Annick M. Persinger, California Bar No. 272996
apersinger@tzlegal.com
TYCKO & ZAVAREEI LLP
10880 Wilshire Boulevard
Suite 1101
Los Angeles, CA 90024

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Telephone: (510) 254-6808

*Attorneys for Plaintiffs and the Proposed Class
and Subclasses*